How Cisco IT Uses Firewalls to Protect Cisco Internet Access Locations

Cisco PIX Security Appliance provides stateful firewall protection at smaller Internet gateways.

BUSINESS BENEFITS

- Increased security
- Higher availability
- Configuration time cut by half
- Reduced rack space requirements

"The Cisco PIX Security Appliance has helped us achieve our goals for business continuity and simplified management in the small POP environment … and we'll extend the same benefits to our larger sites."

– Hasan Talukdar, Cisco IT Network Engineer

Recently, Cisco® IT began deploying gateways at data centers to better support remote-access VPN connectivity. Employees working remotely needed improved access to the company intranet, to link them directly to the nearest Cisco VPN gateway instead of sending packets by circuitous routes on the Internet. While connecting to the Internet brought increased employee productivity, it also brought increased risk and required protection. Cisco IT selected the Cisco PIX® 535 Firewall and the Cisco PIX 525 Security Appliance to deploy in all Internet gateways.

The main advantage available on the Cisco PIX Security Appliance is stateful inspection. A stateful-inspection firewall remembers the state of a network connection passing through one direction, so that when the flow returns in the other direction, the firewall recognizes it and passes it through to its destination. The firewall expects to see the return traffic and forwards it without having to check the rules, thus eliminating the need to maintain a second set of ACLs.

The deployment of the Cisco PIX Security Appliance improved application availability via its stateful failover capability. Cisco equipped six internet gateway locations worldwide with redundant PIX security appliances. Should the primary appliance fail, the secondary device takes control so that no packets are lost. Another way the Cisco PIX Security Appliance ensures availability is by performing the Port Address Translation (PAT) function more efficiently than a dedicated gateway.

The Cisco PIX Security Appliance provides an additional layer of security by examining packet streams at layers 4 through 7, and Network-Based Application Recognition (NBAR) is used to defend against the spreading of worms and viruses. Moreover, the security appliance remembers the state of TCP, UDP, or ICMP flow, thus preventing a would-be intruder from inserting another flow.

Cisco IT has achieved its goal of reducing configuration time by half, because the Cisco PIX Security Appliance automatically allows the return traffic for both incoming and outgoing ACLs and rules. The Security Appliance also eliminates the need to configure the secondary router separately: the configuration for the primary firewall is saved to the secondary over a failover cable. This reduces the likelihood of errors and saves administrative overhead.

Cisco has reduced its data center rack space requirements, by replacing the Cisco 7200 Series routers with the smaller Cisco PIX 525 Security Appliance: this device is a two rack unit, compared to three units for the previous router. That's important in our data center, where rack space is at a premium.

The Cisco PIX 525 Security Appliance reduces the IT burden by half.

Case Study: http://www.cisco.com/web/about/ciscoitatwork/case_studies.html

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**